INTERNATIONAL STANDARD

ISO/IEC 27050-3

First edition
2017-10

Information technology — Security techniques — Electronic discovery —

Part 3: Code of practice for electronic discovery

Technologies de l'information — Techniques de sécurité — Découverte électronique —
Partie 3: Code de pratique pour la découverte électronique

Reference number
ISO/IEC 27050-3:2017(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

A list of all parts in the ISO/IEC 27050 series can be found on the ISO website.

Introduction

This document provides requirements and guidance associated with the electronic discovery process elements described in ISO/IEC 27050-1. While the requirements and recommendations are not intended to contradict or supersede local jurisdictional laws and regulations, they are expected to be useful for both legal and non-legal application, as well as for both technical and non-technical personnel involved in some or all of the electronic discovery activities. Additional materials are provided to help organizations better understand the objectives associated with each electronic discovery process element and considerations to avoid failures, which can mitigate risk and expense if electronic discovery becomes an issue.

Electronic discovery often serves as a driver for investigations, as well as evidence acquisition and handling activities (covered in ISO/IEC 27037). In addition, the sensitivity and criticality of the data sometimes necessitate protections like storage security to guard against data breaches (covered in ISO/IEC 27040).

Note that this document is not a reference or normative document for regulatory and legislative security requirements. Although it emphasizes the importance of these influences, it cannot state them specifically, since they are dependent on the country, the type of business, etc.

Information technology — Security techniques — Electronic discovery —

Part 3: Code of practice for electronic discovery

1 Scope

This document provides requirements and guidance on activities in electronic discovery, including, but not limited to, identification, preservation, collection, processing, review, analysis and production of electronically stored information (ESI). In addition, this document specifies relevant measures that span the lifecycle of the ESI from its initial creation through to final disposition.

This document is relevant to both non-technical and technical personnel involved in some or all of the electronic discovery activities. It is important to note that the requirements and guidance are not intended to contradict or supersede local jurisdictional laws and regulations and it is expected that care is exercised by the user to ensure compliance with the prevailing jurisdictional requirements.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27050-1:2016, *Information technology — Security techniques — Electronic discovery — Part 1: Overview and concepts*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and ISO/IEC 27050-1 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at http://www.iso.org.obp

— IEC Electropedia: available at http://www.electropedia.org/

4 Abbreviated terms

ESI Electronically stored information

ICT Information and communications technology

OCR Optical character recognition

5 Electronic discovery background

Electronic discovery is an element of traditional discovery and it is a process that typically involves identifying, preserving, collecting, processing, reviewing, analysing, and producing electronically stored information (ESI) that may be potentially relevant to a particular matter. The requirements and recommendations provided in this document are in accordance with the electronic discovery concepts described in the following clauses and subclauses of ISO/IEC 27050-1.

— Clause 3, Terms and definition: Key electronic discovery terminology

— 6.2, Basic concepts: Electronic discovery issues and primary cost drivers

— 6.3, Objectives of electronic discovery: General electronic discovery objectives

— Clause 7, Electronically stored information (ESI): Common ESI types, common sources and representations

— Clause 8, Electronic discovery process: Description of the electronic discovery process and the process elements

ISO/IEC 27050-1 differentiates between generic actions such as "identifying" from the specific electronic discovery process elements by preceding the names with "ESI" (e.g. ESI identification). Likewise, this document follows this approach. Figure 1, repeated from ISO/IEC 27050-1, shows all of the electronic discovery process elements and the interrelationships between them (see ISO/IEC 27050-1:2016, 8.1 for a full description).

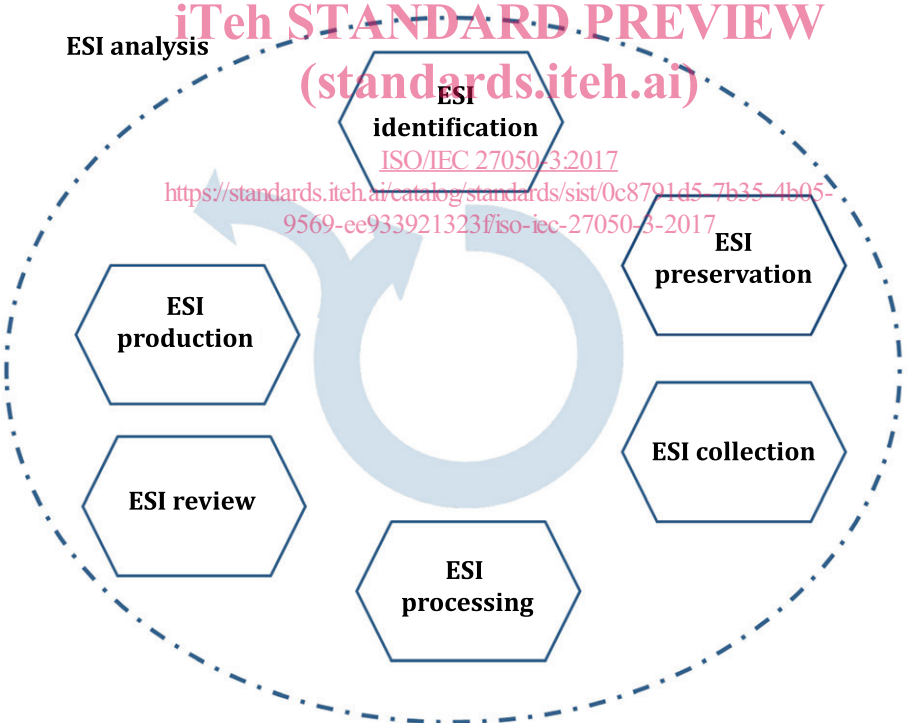

Figure 1 — Electronic discovery process elements

Although the goal of electronic discovery is the same as with hardcopy document discovery — to find and to produce information that is potentially relevant in a matter — the nature of electronic information adds differing layers of complexity and opportunity, since ESI carries with it such elements as metadata and requisite data processing and management functions that do not exist with paper. In addition, the collection and processing of ESI for discovery presents challenges (e.g. data corruption, password protection, encryption, indexing issues, inadequate keyword search, poor OCR) that may have importance either to the viability or accuracy of the ESI produced to the opposing side or to the

ability to maintain provenance or chain of custody. Further, the escalating volumes of ESI typically created, maintained and collected present challenges for consistency and accuracy in review.

This document addresses these challenges by:

— promoting common understanding of various concepts and terminology for electronic discovery;

— articulating objectives and risks inherent in the steps in the electronic discovery process;

— encouraging practical and cost-effective discovery by those tasked with managing ESI through the process;

— providing guidance and best practices for those responsible for delivering electronic discovery projects (e.g. legal practitioners, services providers, independent experts, courts, and any other parties engaged in the process);

— identifying competency areas for those involved in electronic discovery;

— promoting the proactive use of technology to reduce costs and risks, while increasing efficiencies throughout the discovery process;

— suggesting ways to avoid inadvertent disclosures of potentially privileged, confidential, or sensitive ESI.

The overriding goal is to help organizations meet their electronic discovery goals (e.g. legal obligations, business objectives, regulatory requirements).

While this document has been written with larger electronic discovery projects in mind, and therefore covers aspects encountered in the majority of matters, it is not necessarily the case that all steps will be required or proportionate to every matter. For example, in small matters, it may well be that a single person manages and completes every aspect of the project, whereas larger matters may warrant the use of separate individuals or even teams for each element of the electronic discovery project.

6 Electronic discovery requirements and guidance

6.1 Overview

6.1.1 Structure of materials describing the process elements

Each electronic discovery process element is addressed in a separate clause and each contains the following:

a) an overview of the process element;

b) objectives for the process element;

c) considerations to avoid failures;

d) the requirements and guidance specific for the process element.

The order of the clauses in this document does not imply their importance or a particular sequence that needs to be followed.

6.1.2 Cross-cutting aspects

Cross-cutting aspects are behaviours or activities that span multiple electronic discovery process elements and need to be coordinated across the process elements.

— **Planning**. To be effective, most or all of the process elements need to be well planned from the outset, with the specific objectives and conditions taken into consideration and with the resources to be deployed readily available.

— **Transparency**. Implementation of the process elements often necessitates refinement and iteration that have to be readily explained to interested parties. An effective process will be dependent on transparency, as well as allowing for changes and for explanation later on.

— **Documentation**. The process elements need to be well documented, both for the purpose of defending the scope and activities of the process elements down the line if they are challenged, and for the purpose of improving the effectiveness and consistency of future implementations of the process elements.

— **Expertise**. Certain kinds of specialized expertise and qualifications will be necessary for each process element to do the work and to meet any operative standards. This expertise can be associated with the matter at hand, language, technology, the chosen tools or methods, or the quality assurance of the results of applying those tools and methods.

— **Informed**. An effective electronic discovery process is dependent on the pertinent legal and subject matter experts being well informed as to the purposes to be served by the relevant process elements, the relevant requirements (e.g. operative, matter-specific, process-specific, etc.), and the landscape of the ESI, as well as having an understanding of the subject matter, scope and timeframe that apply to the situation in question.

— **Adaptive**. Almost all electronic discovery projects begin in a state of imperfect knowledge when requirements and definitions are not yet fully specified and the ESI landscape is not yet fully mapped. Adaptability is therefore an essential feature of an effective electronic discovery process in general.

— **Use of technology.** The effectiveness of an electronic discovery project can be dependent on how it avails itself of the tools and methods appropriate to the general approach taken in the various process elements; the specific tools and methods can vary from one approach to the other, but most approaches can benefit from the appropriate application of technology.

6.2 ESI identification

6.2.1 Overview of ESI identification

In this subclause, the objectives of ESI identification, the issues inherent in that process element, and considerations to avoid failures are discussed.

ESI may need to be identified and preserved in an organization for a number of reasons, including reasonable anticipation of a lawsuit, receipt of a pre-litigation preservation request, a request to inspect, a demand letter, a cease and desist letter, a cure notice, or even a discussion with an opposing party or its counsel. In some jurisdictions, courts, legislatures, or government regulators have developed rules concerning how organizations identify ESI, particularly for purposes of civil and criminal proceedings, investigations and audits. As a result, it is advisable for organizations to understand when a duty (or need) to preserve is triggered and any steps that may have been mandated or accepted as best practices to identify and preserve relevant ESI in jurisdictions in which they do business.

ESI identification is the element in the electronic discovery process in which information that could be potentially relevant to a matter is specifically located for potential preservation or collection.

6.2.2 Objectives for ESI identification

As defined in ISO/IEC 27050-1, ESI identification is the “element of an electronic discovery process focused on locating potential sources and the criteria for selecting potentially relevant electronically stored information.” A primary objective of ESI identification often is to identify key departments, individuals, custodians, and locations of ESI or ESI sources that could reasonably lead to the discovery of potentially relevant information related to the subject matter in question. In order to undertake such ESI identification, an organization needs to be able to:

— understand the nature of the subject matter in question;

— identify individuals who may have or know relevant information;

— know the potential ESI sources likely to contain such information;

— identify potentially relevant information with a level of accuracy appropriate to the circumstances;

— identify potentially relevant information within a timeframe that is consistent with the overall electronic discovery objectives; and

— accomplish the above tasks with a level of resource utilization that is proportionate to what is at stake in the matter that has necessitated the effort.

6.2.3 Considerations to avoid failures

The primary issues associated with ESI identification are the following:

— **Destruction of ESI by untimely delay.** A delay in locating potentially relevant ESI could result in the inadvertent destruction of the ESI. Such inadvertent destruction could occur if custodians have not been properly advised to refrain from deleting ESI related to relevant subject matter, or when there is, by company policy, a routine deletion policy in place for certain data stores (e.g. a 90-day retention cycle for email).

— **Incomplete or erroneous identification of ESI.** An incomplete or erroneous identification of custodians and sources can result in delays or cost-overruns and, in the context of legal proceedings, legal consequences if a late production unreasonably hinders a case. Defensibility of ESI identification may be questioned and, depending on jurisdiction, documentation and quality control procedures may be scrutinized.

The issues identified above can be managed via the implementation of a process that makes well-coordinated use of appropriate individuals, tools, methods, and expertise in order to meet the defined ESI identification objectives. More specifically, the issues can be managed by the implementation of an ESI identification process that adheres to the following principles:

— **Organized.** Certain kinds of specialized expertise may be called for in ESI identification, whether subject matter experts or the ICT personnel who manage implicated ESI or those with knowledge to query systems to assess system relevance. A plan that identifies from the outset the kinds of expertise required and contains interview templates and other tools to document the information learned can be very helpful. An organization would be wise to identify a team of key people that need to be involved in discovery project management, including ESI identification. These individuals typically include corporate legal counsel, outside counsel, ICT personnel, records management personnel, data custodians, human resources personnel, business leaders, and service providers/electronic discovery consultants.

— **Planned.** To be effective, an ESI identification process needs to be well planned from the outset, with the specific objectives and conditions taken into consideration and with the resources to be deployed readily available. Being proactive and gathering timely information about custodians and existing systems can enable an organization to meet the expectations of the courts and regulators. An effective ESI identification process is typically well informed by individuals with the appropriate expertise who are aware of the requirements of identifying and collecting potentially responsive ESI. A well-planned ESI identification makes provision for quality-control assessments that monitor progress and completeness of the plan as it is being executed. An effective plan also provides timelines and cost targets that can realistically be met and are appropriate to the matter.

— **Transparent.** Implementation of ESI identification often necessitates refinement and iteration that may have to be explained to interested parties. An effective process will be dependent on transparency, as well as allowing for changes and for explanation later on. A transparent process is one in which identified steps are clearly communicated and evidence of their execution as described is documented. Since ESI identification can be iterative in that additional individuals and new sources of potentially responsive information can be added as more is known, it is important to document such changes as they occur. To that end, in order for the process to be transparent,

tools that document processes and capture information during ESI identification (e.g. custodian interview templates) are useful if explanation is required later.

— **Documented.** As ESI identification proceeds, organizations need to be prepared to adequately document the process to be able to show that reasonable steps were taken to identify potentially responsive information. Such documentation is especially important considering that some litigation can go on for years and still require a look-back at steps that were initially taken to identify potentially responsive information.

6.2.4 Requirements for ESI identification

ESI identification carries significant importance. Since it occurs early and essentially defines the universe of potentially relevant hardcopy documents or ESI, missteps can result in significant problems later on. At best, additional collections can ensue, with additional collection, processing and review costs and delays. In the context of legal proceedings, if key individuals or ESI sources have been overlooked or ESI has been deleted, claims with potential legal consequences can result in some jurisdictions.

The best way to avoid these problems is with a plan that includes the individuals, ESI sources, tools and procedures that can be deployed if information in the enterprise needs to be identified.

The following are requirements for ESI identification.

a) The ESI identification coordinator shall be informed as to the purposes to be served by the identification effort and develop an understanding of the subject matter, scope and timeframe that apply to the situation in question.

b) The individuals responsible for identification of potentially relevant ESI shall, in advance of executing ESI identification, develop a plan to guide the identification effort.

c) The individuals executing the identification process shall be informed with regard to operative requirements that govern ESI identification including:

   1) legal requirements,

   2) matter-specific requirements,

   3) process-specific requirements, and

   4) the landscape of ESI that may be within the scope of the matter.

d) ESI identification shall be sufficiently transparent during its implementation to enable the individuals responsible for identification to assess its progress and make adjustments as warranted.

e) ESI identification shall be supported by appropriate methods and metrics.

f) ESI identification shall be adapted, as needed, to changes in the requirements that govern the identification effort and by any additional information obtained during the identification process, such as addition of knowledgeable custodians, relevant ESI sources, or aspects of the ESI environment that may be pertinent (e.g. auto-delete functions).

g) The identification procedures implemented shall be documented to accurately reflect:

   1) all procedures followed in the course of identification,

   2) all significant decisions made during the identification process, and

   3) any evaluations of the effectiveness of the identification process.

